



Billing Code: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2015-OS-0044]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary of Defense, DoD.

ACTION: Notice to add a New System of Records.

SUMMARY: The Office of the Secretary of Defense proposes to add a new system of records, DMDC 19 DoD, entitled "Secure Web Fingerprint Transmission (SWFT)" to its inventory of record systems subject to the Privacy Act of 1974, as amended. This system will provide a means for all DoD individuals required to submit electronic fingerprints and demographic information to the Office of Personnel and Management (OPM) and the Federal Bureau of Investigation (FBI) for a personnel security clearance or as part of a background investigation.

Additionally, SWFT will transmit an electronic fingerprint file with demographic information as part of a background investigation to the Defense Manpower Data Center (DMDC) Person Data Repository (PDR) for identity matching purposes.

DATES: Comments will be accepted on or before **[INSERT 30-DAYS FROM DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This

proposed action will be effective the day following the end of the comment period unless comments are received which result in a contrary determination.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

- * Federal Rulemaking Portal: <http://www.regulations.gov>.
Follow the instructions for submitting comments.

- * Mail: Department of Defense, Office of the Deputy Chief Management Officer, Directorate of Oversight and Compliance, Regulatory and Audit Matters Office, 9010 Defense Pentagon, Washington, DC 20301-9010.

Instructions: All submissions received must include the agency name and docket number for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at <http://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ms. Cindy Allard, Chief, OSD/JS Privacy Office, Freedom of Information Directorate, Washington Headquarters Service, 1155 Defense Pentagon, Washington, D.C. 20301-1155, or by phone at (571)372-0461.

SUPPLEMENTARY INFORMATION: The Office of the Secretary of Defense notices for systems of records subject to the Privacy

Act of 1974 (5 U.S.C. 552a), as amended, have been published in the Federal Register and are available from the address in FOR FURTHER INFORMATION CONTACT or at <http://dpclld.defense.gov/>

The proposed system report, as required by 5 U.S.C. 552a(r) of the Privacy Act of 1974, as amended, was submitted on May 5, 2015, to the House Committee on Oversight and Government Reform, the Senate Committee on Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to paragraph 4c of Appendix I to OMB Circular No. A-130, "Federal Agency Responsibilities for Maintaining Records About Individuals," dated February 8, 1996 (February 20, 1996, 61 FR 6427).

Dated: May 8, 2015.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

DMDC 19 DoD

System name:

Secure Web Fingerprint Transmission (SWFT).

System location:

Defense Manpower Data Center, DoD Center Monterey Bay, 400
Gigling Road, Seaside, CA 93955-6771.

Categories of individuals covered by the system:

DoD military, civilian, and contractor personnel, and non-Federal agency civilian associates (e.g., American Red Cross paid employees, state employees supporting National Guard) eligible for the Common Access Card.

Categories of records in the system:

Social Security Number (SSN), name, place of birth, date of birth, electronic fingerprint file.

Authority for maintenance of the system:

DoD Directive 5105.42, Defense Security Service (DSS); DoD Instruction 5200.02, DoD Personnel Security Program (PSP); 32 CFR part 156, Department of Defense Personnel Security Program (DODPSP); E.O. 10450, Security requirements for Government employment; HSPD 12, Policy for a Common Identification Standard for Federal Employees and Contractors; and E.O. 9397 (SSN), as amended.

Purpose:

To provide a means for all DoD individuals required to submit electronic fingerprints and demographic information to the Office of Personnel and Management (OPM) and the Federal Bureau of Investigation (FBI) for a personnel security clearance or as part of a background investigation.

Additionally, SWFT will transmit an electronic fingerprint file with demographic information as part of a background investigation to the Defense Manpower Data Center (DMDC) Person Data Repository (PDR) for identity matching purposes.

Routine uses for records maintained in the system including categories of users and the purposes of such uses:

In addition to disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained herein may specifically be disclosed outside the DoD as follows to:

The Office of Personnel and Management (OPM) and the Federal Bureau of Investigation (FBI) for investigative purposes related to the conduct of security clearance investigations and background checks.

The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense (OSD) compilation of systems of records notices may apply to this system. The complete list of DoD blanket routine uses can be found online at:

<http://dpclld.defense.gov/Privacy/SORNSindex/BlanketRoutineUses.aspx>

Policies and practices for storing, retrieving, accessing, retaining and disposing of the records in the system:

Storage:

Electronic storage media.

Retrievability:

SSN and/or name.

Safeguards:

Electronic records are maintained in a controlled area accessible only to authorized personnel. Entry to these areas is restricted by the use of locks, guards, and administrative procedures. Electronic data are stored in an encrypted database. Access to personal information is limited to those who require the records in the performance of their official

duties. Access to personal information is further restricted by the use of passwords which are changed periodically.

Retention and disposal:

Electronic fingerprints are destroyed/deleted three (3) year(s) after successful transmission.

Unsuccessfully transmitted electronic fingerprints are destroyed/deleted when 90 days old.

System manager(s) and address:

Deputy Director for Identity and Personnel Assurance, Defense Manpower Data Center, 4800 Mark Center Drive, Alexandria, VA 22350-6000.

Notification procedure:

Individuals seeking to determine whether information about themselves is contained in this system should send written inquiries to: SWFT Program Manager, Personnel Security and Assurance Division, Defense Manpower Data Center, 400 Gigling Road, Seaside, CA 93955-6771.

Signed, written requests must contain the full name and SSN of the subject individual, along with a return address.

Record access procedures:

Individuals seeking access to information about themselves contained in this system must send signed written inquiries to: Office of the Secretary of Defense/Joint Staff Freedom of information Act Request Service Center, 4800 Mark Center Drive, Alexandria, VA 22350-3100.

Signed, written requests must contain the full name and SSN of the individual and address where the records are to be returned.

Contesting records procedures:

The OSD rules for accessing records, contesting contents, and appealing initial agency determinations are contained in OSD Administrative Instruction 81; 32 CFR part 311; or may be obtained from the system manager.

Record source categories:

Individual, industrial facilities cleared by the Personnel Security Management Office for Industry (PSMO-I), and DoD Component fingerprint capture devices.

Exemptions claimed by the system:

None.

[FR Doc. 2015-11606 Filed: 5/13/2015 08:45 am; Publication
Date: 5/14/2015]